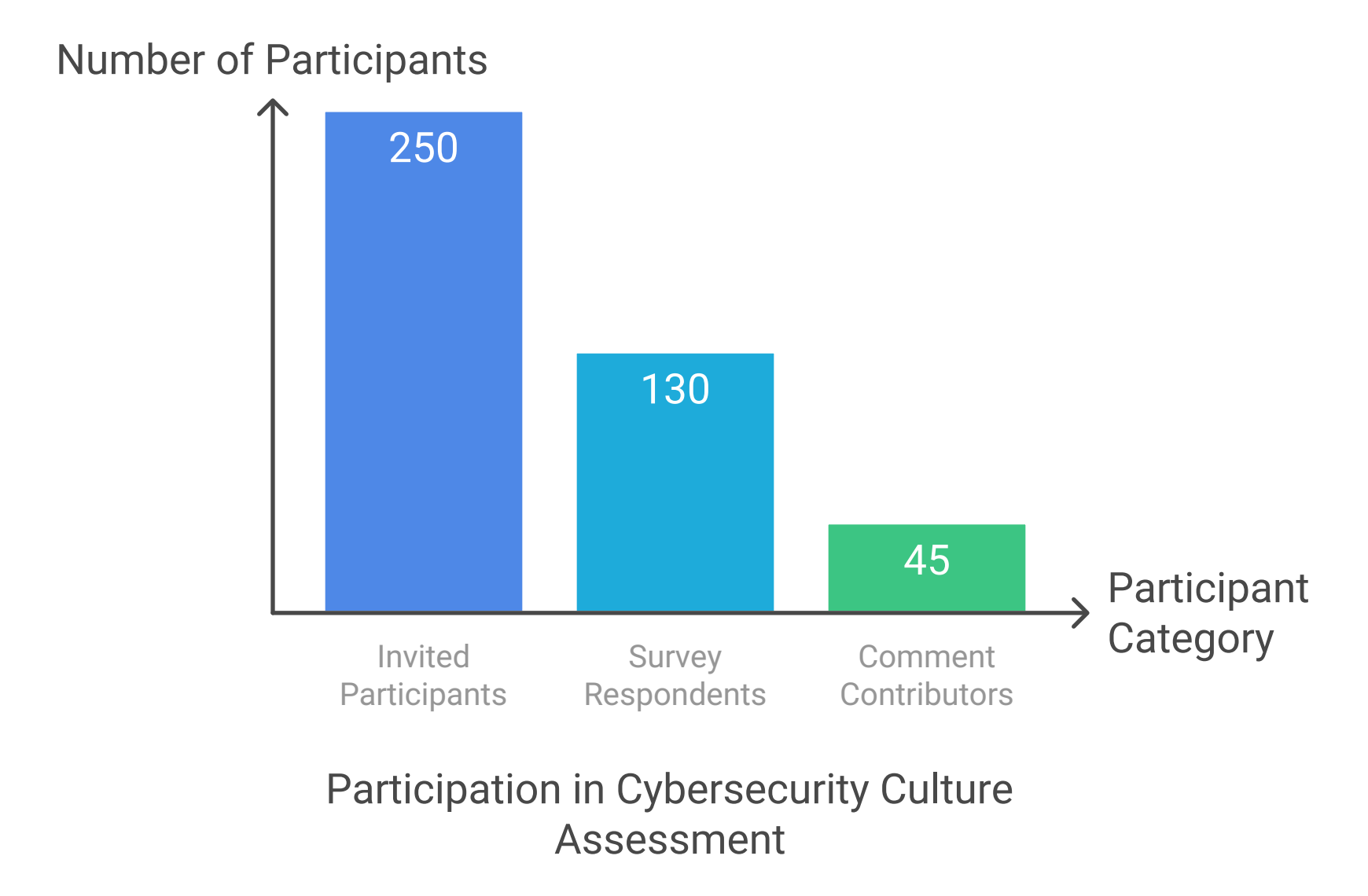
Cybersecurity Culture at Zenith Solutions: Recommendations and Action Plan

1. Introduction

This report presents the findings from the cybersecurity culture assessment conducted at Zenith Solutions. The purpose of this assessment was to understand the current cybersecurity mindset among employees, identify strengths and areas for improvement, and provide guidance on how to enhance the organization's overall security posture. By clarifying the scope, methodology, and participation rates, as well as offering prioritized, data-driven recommendations, this report aims to empower leadership—particularly the Chief Information Security Officer (CISO)—to make informed decisions that advance Zenith' cybersecurity culture.

Participation and Response Rates:
- **Invited Participants:** 250 employees across all departments were invited to participate in the assessment.
- **Survey Respondents:** 130 employees completed the survey, resulting in a response rate of 52%.
- **Comment Contributors:** Of those respondents, 45 provided open-ended comments, offering qualitative insights into the organization's cybersecurity culture.

The assessment involved a 20-question anonymous online survey, which garnered responses from 130 out of 250 invited employees (52%). Additionally, qualitative comments were analyzed through thematic coding and sentiment analysis. The findings revealed both positive aspects and areas of concern regarding the organization's cybersecurity culture.



High Priority: Improve VPN Performance

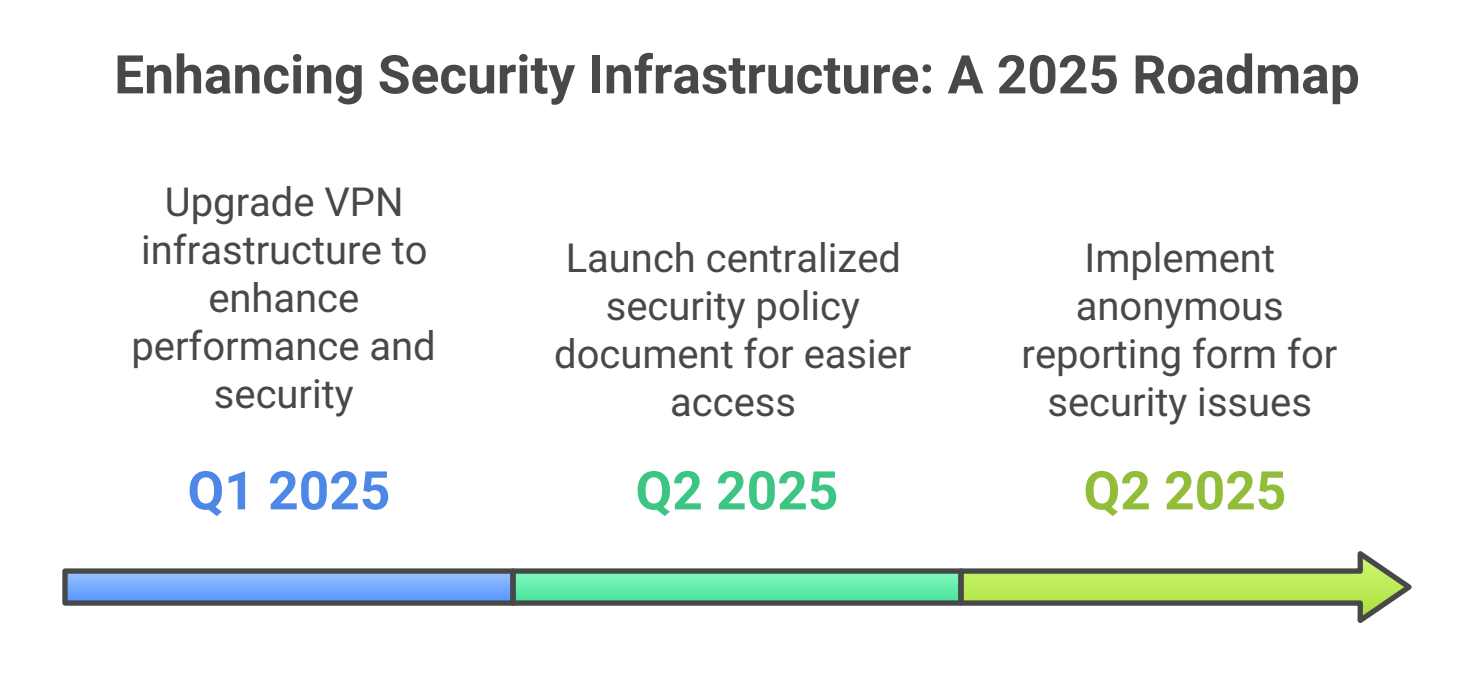
- **Linked Finding**: Slow VPN causes insecure data handling.
- **Action**: Upgrade VPN infrastructure by Q1 2025 to enhance performance and security.
- **Metric**: Achieve a 100% reduction in reports of local data copies post-implementation.

Medium Priority: Centralized Security Portal

- **Linked Finding**: Employees want easier access to security policies and resources.
- **Action**: Launch and communicate a centralized security policy document by Q2 2025 to enable access.
- **Metric**: Target a 80% accept increase in document visits and a 15% rise in policy quiz completions.

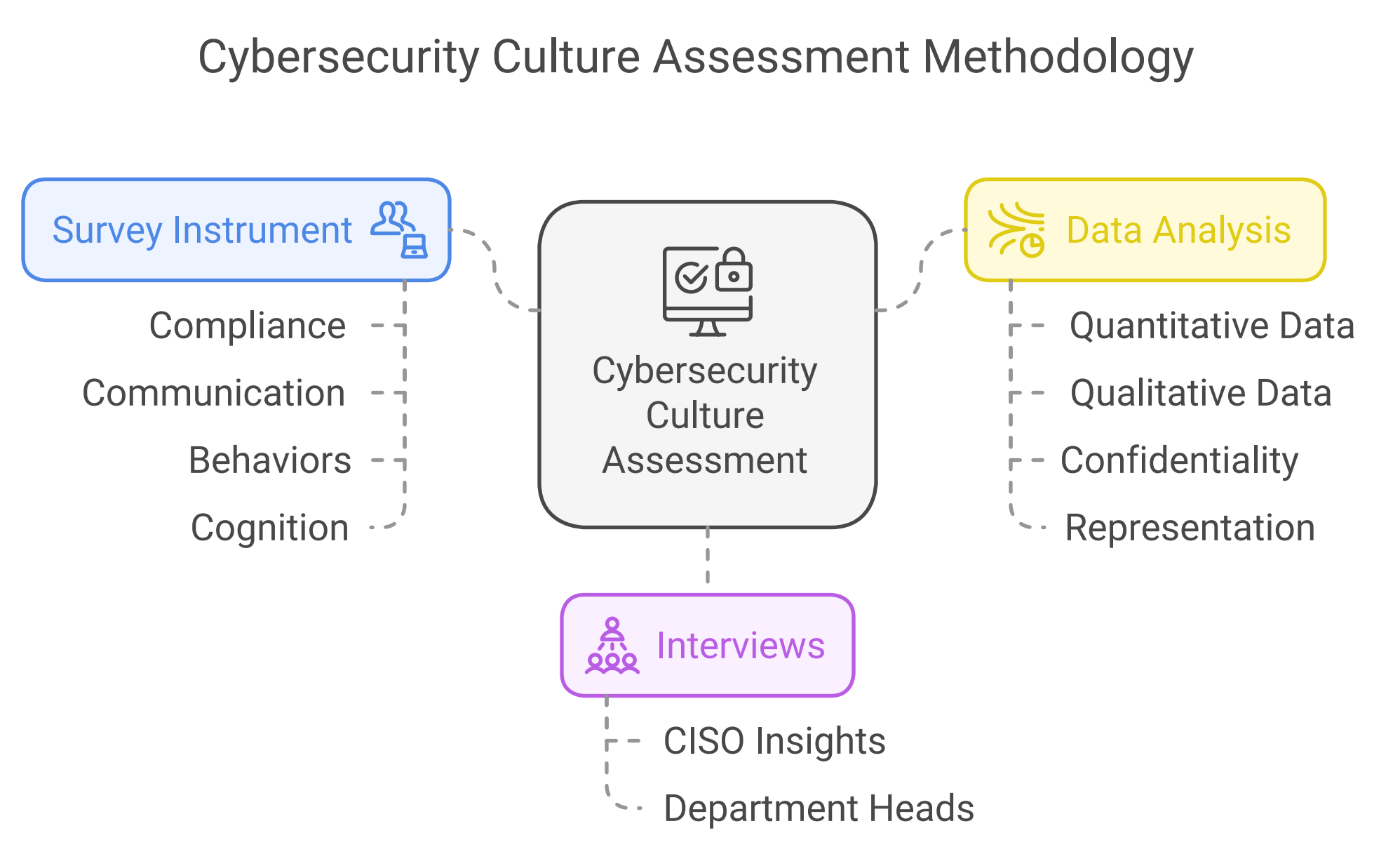
Low Priority: Streamlined Security Reporting

- **Linked Finding**: Unclear reporting channels beyond phishing incidents.
- **Action**: Implement an anonymous reporting form by Q2 2025 to facilitate reporting of security issues.
- **Metric**: Aim for a 25% increase in reported issues within six months of implementation.



2. Methodology

The assessment employed a mixed-method approach to capture both quantitative and qualitative data.
- **Survey Instrument:** A 20-question anonymous online survey was distributed via the internal communications platform. Questions addressed four core categories: Compliance, Communication, Behaviors, and Cognition. Participants were asked to rate their perceptions on a Likert scale (1–5) and had opportunities to provide open-ended comments.
- **Interviews:** In addition to the survey, the CISO and two department heads participated in structured interviews. These sessions explored deeper insights into leadership's view of the current security culture and areas needing improvement.
- **Data Analysis:**
  - **Quantitative Data:** Likert-scale responses were aggregated to determine average sentiment and identify category-specific strengths and weaknesses.
  - **Qualitative Data:** Open-ended comments were analyzed using a thematic coding approach, assisted by a third-party sentiment analysis tool (e.g., LexiconSoft). Comments were categorized into key themes—Infrastructure & Tools, Policy & Procedures, Training & Awareness, and Cultural Cognition—and scored on a sentiment scale from 1 (negative) to 10 (positive).
- **Confidentiality and Representation:** The survey was anonymous, and participation was voluntary. Invitations were sent organization-wide to ensure representation across departments such as R&D, Operations, Sales, and Support.



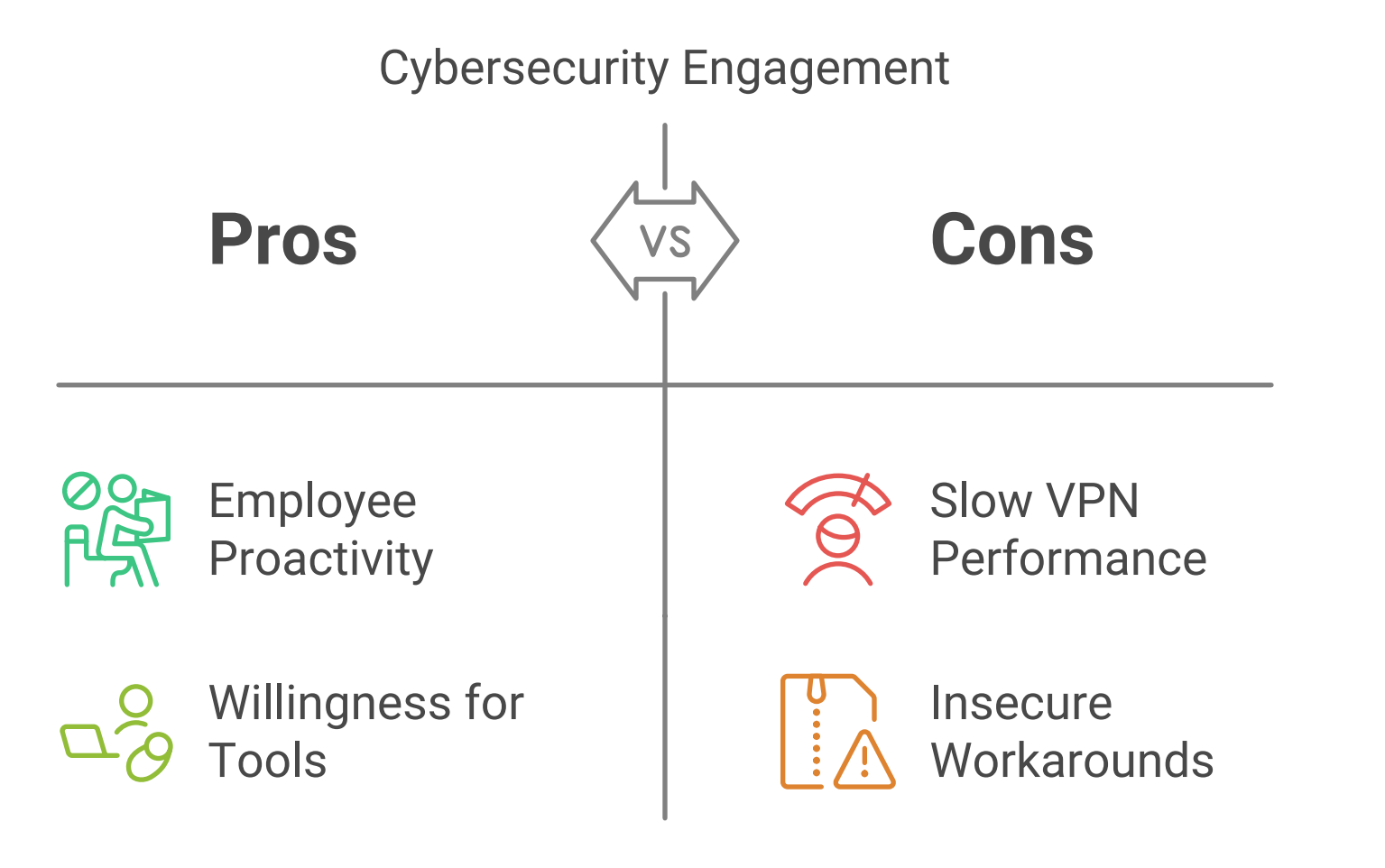
3. Key Findings

Positive Highlights:
- **Acknowledgment of Employee Responsibility (Sentiment: 6.0)***Comment Example:*"We should be encouraged to read through the policies periodically. It would also be beneficial if we would have a portal or landing page for reading various important documents such as the handbook, security best practices, etc."

- *Interpretation:*Employees recognize the importance of their role in maintaining cybersecurity and are receptive to new tools or platforms that streamline their access to policies and resources.

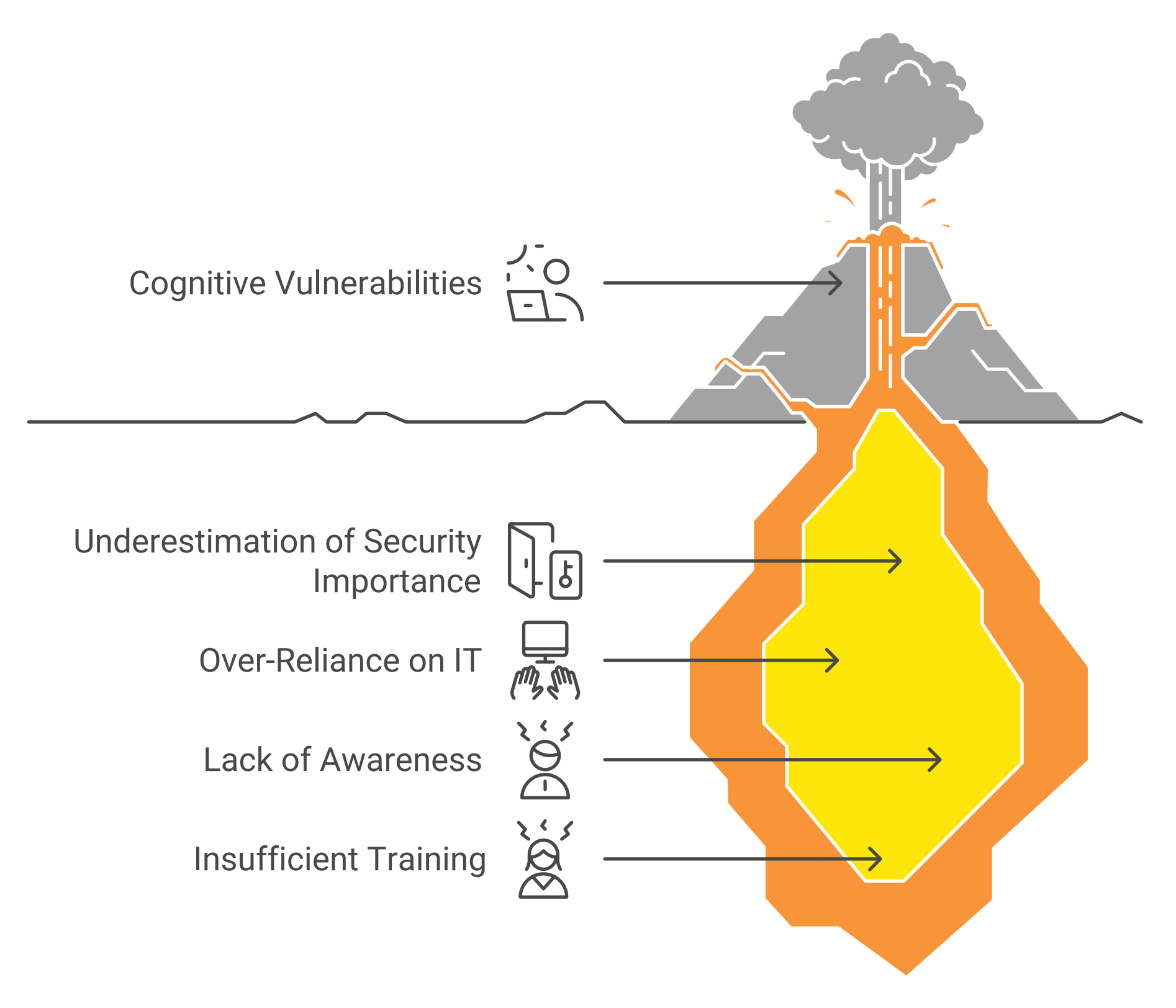
Areas of Concern:
- **VPN Performance (Sentiment: 3.0)***Comment Example:*"VPN connection is so slow that we need to copy content to our computer instead of editing content where it's stored. That leaves copies of documentation everywhere."

- *Interpretation:*Poor VPN performance encourages insecure workarounds (e.g., local data storage) that increase data leakage risks.



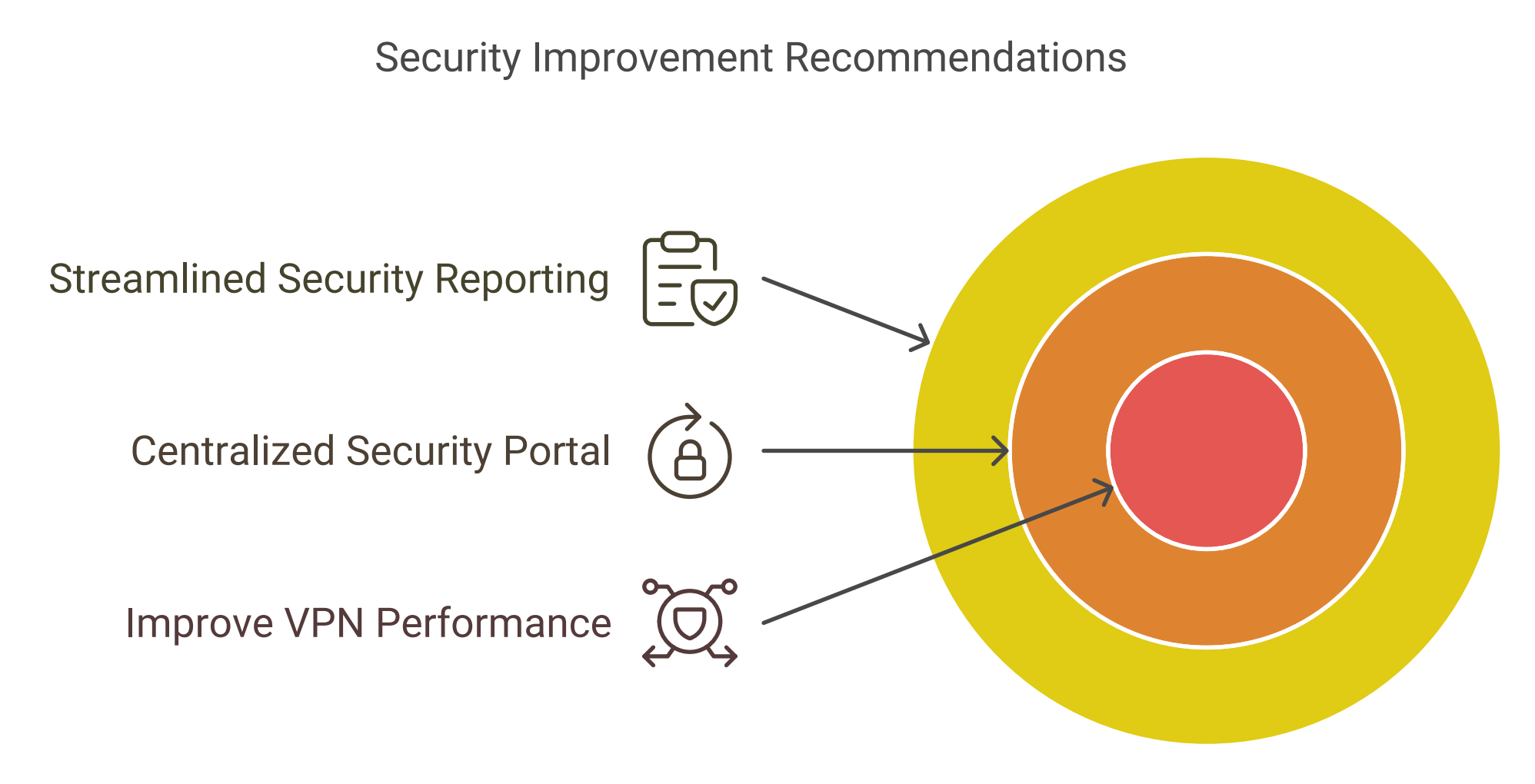
5. Cognitive Vulnerabilities Analysis

Cognitive Vulnerabilities:
- **Underestimation of Security Importance:**
  - *Evidence:* "Security seems like an afterthought."
  - *Impact:* This perception can lead to complacency and lax adherence to best practices.
  - *Preventive Strategy:* Increase visibility of security initiatives through leadership communications and highlight the role each employee plays in safeguarding company data.
- **Over-Reliance on IT for Security:**
  - *Evidence:* "It is always the employee's responsibility to play a role in helping IT keep the company data secure."
  - *Impact:* Employees may view security as IT's sole responsibility, reducing their personal investment in maintaining secure behaviors.
  - *Preventive Strategy:* Provide targeted training sessions and tools that empower employees to identify, report, and mitigate security risks themselves.



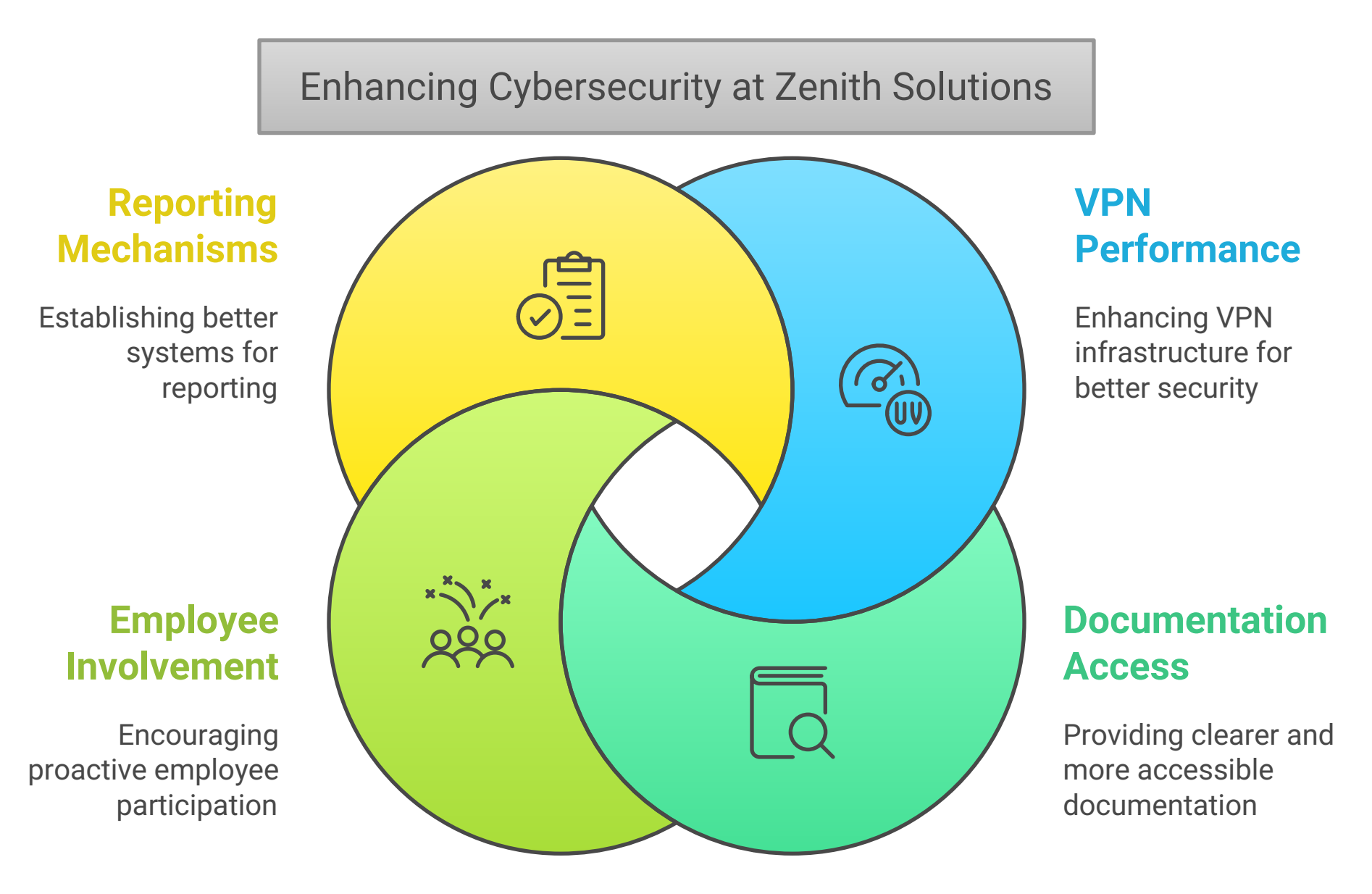
6. Recommendations (with priorities, linked findings, and metrics)

1. **High Priority:** Improve VPN Performance.
   - Linked Finding: Slow VPN causes insecure data handling.
   - Action: Upgrade VPN within Q1 2025.
   - Metric: 20% reduction in local data copies post-implementation.
2. **Medium Priority:** Centralized Security Portal.
   - Linked Finding: Employees want easier policy access.
   - Action: Launch portal by Q2 2025.
   - Metric: 30% increase in portal visits; 15% rise in policy quiz completions.
3. **Low Priority:** Streamlined Security Reporting.
   - Linked Finding: Unclear reporting channels beyond phishing.
   - Action: Anonymous reporting form by Q2 2025.
   - Metric: 25% increase in reported issues within six months.



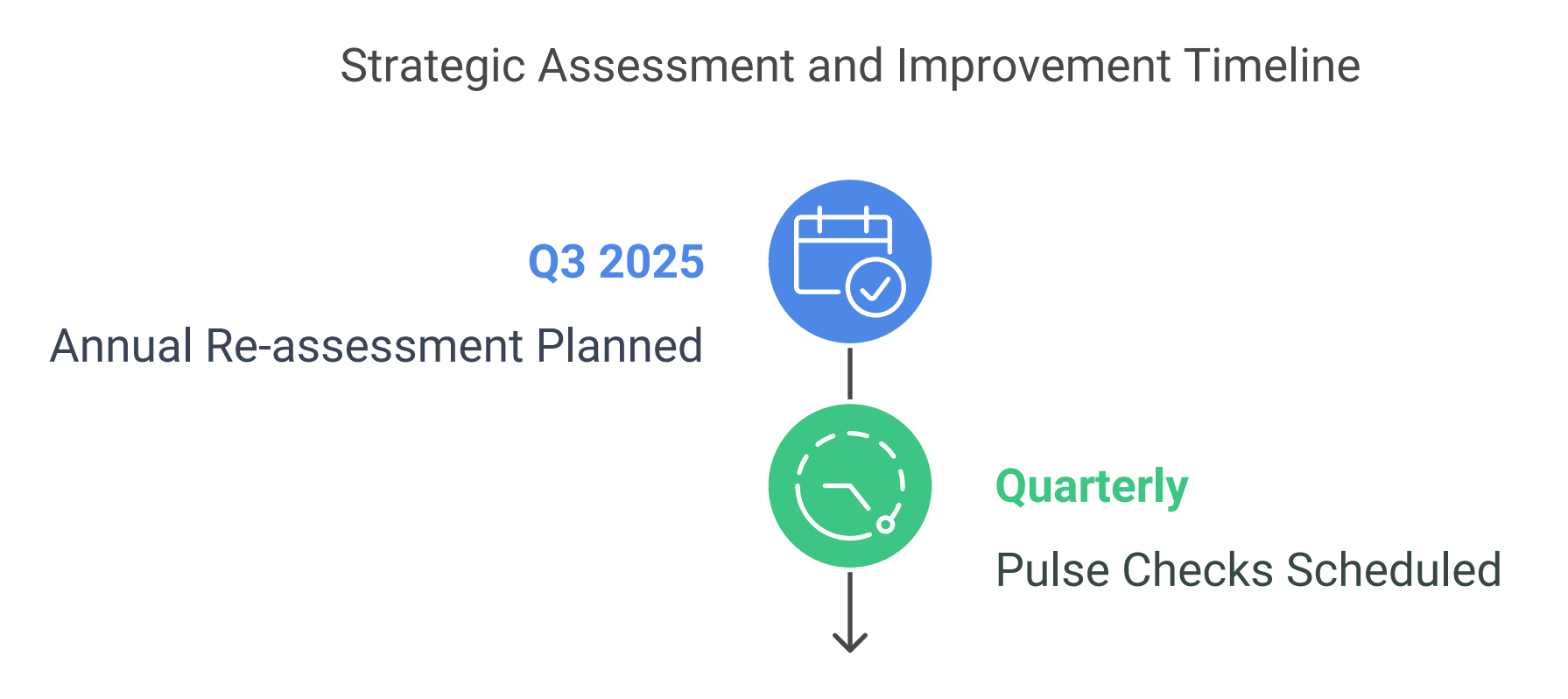
7. Conclusion

This cybersecurity culture assessment indicates that while employees at Zenith generally appreciate the importance of security, there are key opportunities for enhancement. Infrastructure improvements (notably VPN performance), clearer documentation access, more proactive employee involvement, and better reporting mechanisms will strengthen cybersecurity posture. With the recommendations and metrics outlined, leadership can confidently prioritize investments and initiatives that have measurable impact.



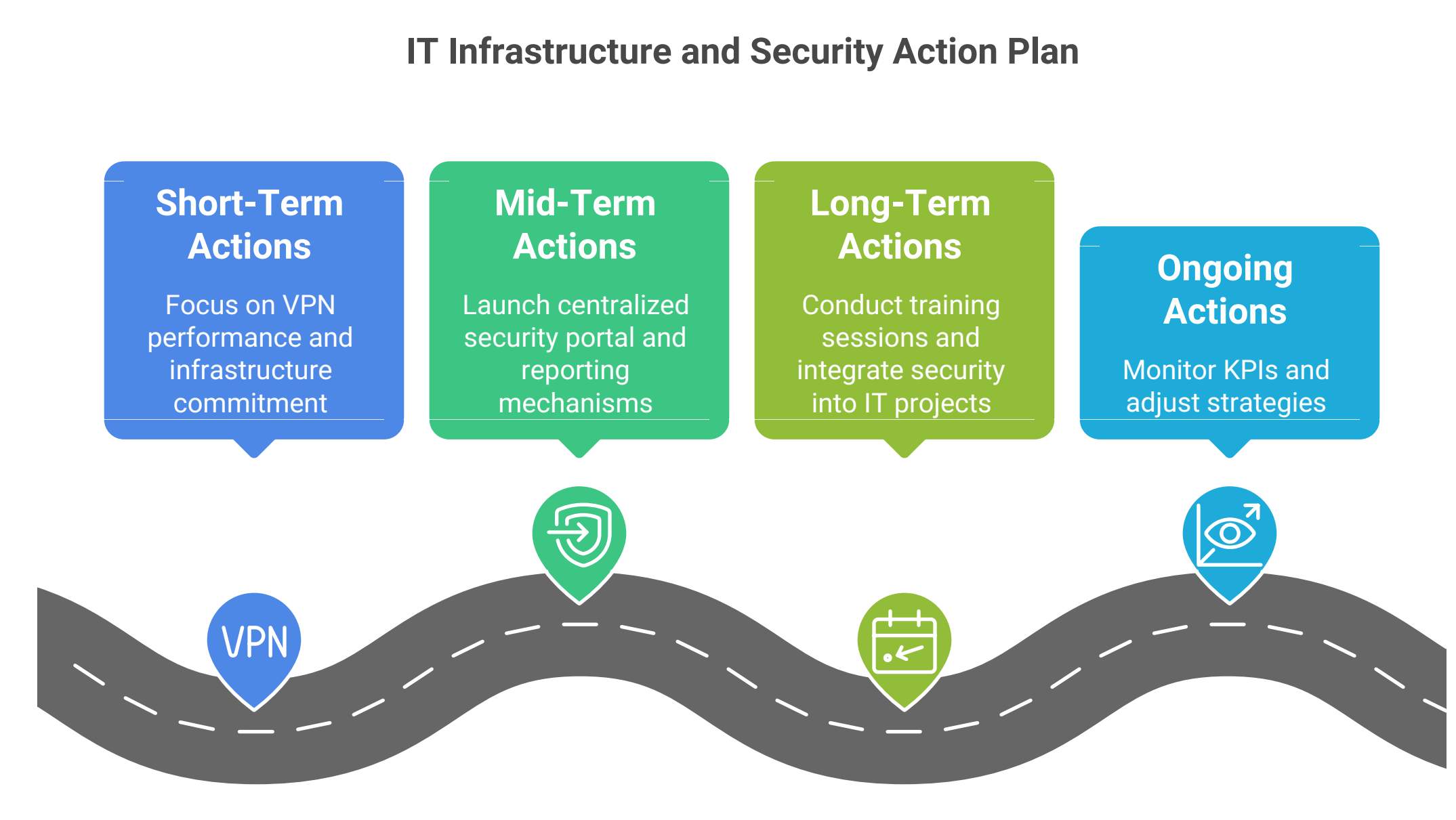
8. Future Assessments

To ensure continuous improvement, an annual re-assessment is planned for Q3 2025, complemented by quarterly pulse checks. These assessments will track progress on the implemented initiatives and guide ongoing strategy refinement.



9. Actions Plan Overview

- **Short-Term (0–3 Months):** Address VPN performance and communicate leadership's commitment to improving infrastructure.
- **Mid-Term (3–9 Months):** Launch the centralized security portal and implement streamlined reporting mechanisms.
- **Long-Term (9–12 Months):** Conduct quarterly training sessions and integrate security considerations into all IT projects.
- **Ongoing:** Monitor KPIs, adjust strategies, and prepare for the next annual assessment cycle.



Ready to Transform Your Cybersecurity Culture?

Discover how these actionable insights can elevate your organization's security posture. For a personalized consultation and tailored strategies, contact us today at info@cyberplate.eu.